M-01-05

December 20, 2000

MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: **Jacob J. Lew /s/**
Director, Office of Management and Budget

SUBJECT: **Guidance on Inter-Agency Sharing of Personal Data – Protecting Personal Privacy**

OMB is issuing guidance to remind agencies of several privacy-related legal requirements that apply to computer matching and to clarify how agencies should conduct computer matching activities. This guidance applies to data matching activities or programs for purposes of establishing or verifying eligibility for Federal benefit programs or recouping payments or delinquent debts under such programs covered by the Computer Matching and Privacy Protection Act ("Matching Act"),[1] an amendment to the Privacy Act of 1974, 5 U.S.C. Section 552a, whether data are shared between Federal agencies or matched with State agency data.[2] Although this guidance applies directly only to programs covered by the Matching Act, agencies should consider applying these principles in other data sharing contexts.

Inter-agency sharing of information about individuals can be an important tool in improving the efficiency of government programs. By sharing data, agencies can often reduce errors, improve program efficiency, identify and prevent fraud, find intended beneficiaries, evaluate program performance, and reduce information collection burden on the public.

As government increasingly moves to electronic collection and dissemination of data, under the Government Paperwork Elimination Act and other programs, opportunities to share data across agencies will likely increase. Agencies should work together to determine what data sharing opportunities are desirable, feasible, and

---

1 For purposes of this guidance, "data sharing" means data matching activities or programs covered under the Computer Matching and Privacy Protection Act.

2 This guidance does not apply to several types of matching activities or programs excluded by the Matching Act, such as matches performed to produce aggregate statistical data without any personal identifiers and matches performed to support any research or statistical project. Such data may not be used to make decisions concerning the rights, benefits, or privileges of specific individuals.

appropriate. In general, data sharing should only be pursued if the benefits outweigh the costs.

With increased focus on data sharing, agencies must pay close attention to handling responsibly their own data and the data they share with or receive from other agencies. When information about individuals is involved, agencies must pay especially close attention to privacy interests and must incorporate measures to safeguard those interests. Prior to any data sharing, agencies must review and meet the Privacy Act requirements for computer matching, including developing a computer matching agreement and publishing notice of the proposed match in the *Federal Register*; OMB Guidance on Computer Matching (54 *Fed. Reg.* 25818, June 19, 1989); and OMB Circular A-130, Appendix I, "Federal Agency Responsibilities for Maintaining Records About Individuals." Agencies must also review and meet applicable requirements under other laws, including the Paperwork Reduction Act of 1995.

The attached memorandum puts forth principles on protecting personal privacy when conducting inter-agency data sharing. Agencies themselves, as well as inter-agency work groups, such as the Chief Financial Officers (CFO) Council, the Chief Information Officers (CIO) Council, the President's Council on Integrity and Efficiency, the Procurement Executives Council (PEC), and the Human Resources Management Council (HRMC) should ensure that they adhere to the principles.

For any questions about this guidance, contact Lauren Steinfeld or Brooke Dickson of the Office of Information and Regulatory Affairs, Office of Management and Budget. Lauren Steinfeld can be reached at phone (202) 395-3647, fax (202) 395-3047, e-mail Lauren_Steinfeld@omb.eop.gov. Brooke Dickson can be reached at phone (202) 395-3191, fax (202) 395-5167, e-mail Brooke_Dickson@omb.eop.gov.

Attachment

ATTACHMENT

Privacy Principles in Conducting Inter-Agency Data Sharing

Existing Requirements

1. Notice.

Agencies that plan to use data sharing to verify program eligibility or to recover delinquent debt should develop procedures for providing notice to the individual at the time of application, and periodically thereafter (as directed by the Data Integrity Board), that the information they provide may be subject to verification through matching programs, as required by the Matching Act. In addition to direct notice to individuals, the Matching Act requires that agencies publish a notice in the Federal Register, at least 30 days before conducting the data match, describing the purpose of the match, the records and individuals covered, and other relevant information.

2. Consent, As Appropriate.

Agencies should obtain the written (or electronic) consent of individuals before sharing personal data protected by the Privacy Act, unless one of the exceptions under Section 552a(b) of the Privacy Act applies.

3. Redisclosure Limitations.

Data sharing programs should prohibit the redisclosure of the data, except as allowed under the Matching Act. Specifically, the Matching Act prohibits recipient agencies, whether Federal or State, from redisclosing records, except where required by law or where the redisclosure is essential to the conduct of the matching program.

4. Accuracy.

Because information shared among agencies may be used to deny, reduce, or otherwise adversely affect benefits to individuals, it is critical that agencies have reasonable procedures to ensure the accuracy of the data shared. At a minimum, this should include providing individuals the right to access and to request amendment of their records, as required by the Privacy Act.

To ensure accuracy, agencies must also adhere to the due process requirements found in the Matching Act. Pursuant to 5 U.S.C. 552a(p), before an agency takes adverse action against an individual based on the results of information produced by a matching

program, it must independently verify the information unless there is a determination by the relevant Data Integrity Board, for a limited class of information, that there is a high degree of confidence that the information is accurate. Agencies must also, at least 30 days before taking adverse action (unless statute or regulation states otherwise), provide notice to the individual of the agency's findings and provide an opportunity to contest those findings. These requirements do not apply in situations where public health or public safety may be adversely affected or significantly threatened.

5. Security Controls.

Agencies should employ adequate and effective security controls to protect the confidentiality, availability, and integrity of all systems and data, including all data shared with other organizations. Agencies should ensure, prior to the sharing of any data, that the recipient organization affords the appropriate equivalent level of security controls as maintained by the originating agency. Since data security remains the responsibility of the originating agency, procedures should be agreed to in advance that provide for the monitoring over time of the effectiveness of the security controls of the recipient organization.

Both originating and recipient agencies should consider and apply all appropriate management, operational, and technical security controls commensurate with the level of risk and magnitude of harm that would occur if the security of the data and the systems that process it were breached. Agencies should particularly consider physical security needs, such as whether personal information is so sensitive that it should be kept in an approved security container, or whether access to where the information is located should be limited. Agencies should also consider personnel security needs, such as additional controls over individuals who have access to data. They should also consider network security, including encryption for data in transit and protection for data at rest. In addition, agencies receiving data via data sharing must have procedures for the retention and timely destruction of identifiable records. Especially for more sensitive data, audit trails and other anti-browsing features may be appropriate in the recipient agency. For further guidance on ensuring adequate security, see OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources" and all associated National Institute of Standards and Technology (NIST) computer security guidance.

Additional Guidance

6. Minimization.

When dealing with paper records, it may be difficult to provide only certain data elements to other agencies, because of the need for manual redaction of other information. In the computer world, it is far easier to implement sharing of only a narrow range of information that is necessary to verify an applicant's eligibility for a program. Agencies should analyze what data are needed for program purposes and make every effort to ensure that they transfer only that information.

7. Accountability.

Data sharing programs should include mechanisms to ensure that agencies are accountable for adhering to these principles. Some of these measures are already found in the Privacy Act, which provides for civil and criminal penalties for non-compliance. Agencies should also consider training programs that stress accountability and explain penalties for breaches of confidentiality. Especially for more sensitive data and more extensive data sharing arrangements, agencies should consider whether additional oversight mechanisms, such as self-audits, are justified.

For example, agencies should establish procedures to ensure compliance with redisclosure limitations. One mechanism for assuring compliance would be to have the recipient agency certify on a periodic basis that it has examined practices regarding redisclosure and, if necessary, taken corrective action where improper redisclosures have occurred.

8. Privacy Impact Assessments.

In the President's FY2001 budget, the President announced an initiative to make "privacy impact assessments," or "PIAs," a regular part of the development of new Government computer systems. A PIA is a plan to build privacy protection into new information systems, such as, for example, by asking systems personnel and program personnel to work through questions on data needs and data protection *before* the system is developed. The CIO Council has voted the IRS PIA a best practice; it is available as a reference at http://www.cio.gov.

For any questions about this guidance, contact Lauren Steinfeld or Brooke Dickson of the Office of Information and Regulatory Affairs, Office of Management and Budget. Lauren Steinfeld can be reached at phone (202) 395-3647, fax (202) 395-3047, e-mail Lauren_Steinfeld@omb.eop.gov. Brooke Dickson can be reached at phone (202) 395-3191, fax (202) 395-5167, e-mail Brooke_Dickson@omb.eop.gov.